(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平9－26975

(43)公開日　平成９年(1997)１月28日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	17/30		9289－5L	Ｇ０６Ｆ	15/40	３２０Ｂ
	12/00	５４５	7623－5B		12/00	５４５Ａ
	13/00	３５７	9460－5E		13/00	３５７Ｚ

審査請求　未請求　請求項の数35　ＯＬ　（全 12 頁）

(21)出願番号　特願平8－143371

(22)出願日　平成８年(1996)６月６日

(31)優先権主張番号　０８／４６９２７６

(32)優先日　1995年６月６日

(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　０８／５１９２６８

(32)優先日　1995年８月25日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ&Ｔ　ＣＯＲＰ.
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(72)発明者　ブレンダ　スエ　ベイカー
アメリカ合衆国　07922　ニュージャーシィ，バークレイ　ハイツ，ノース　ロード　140

(74)代理人　弁理士　岡部　正夫　（外２名）

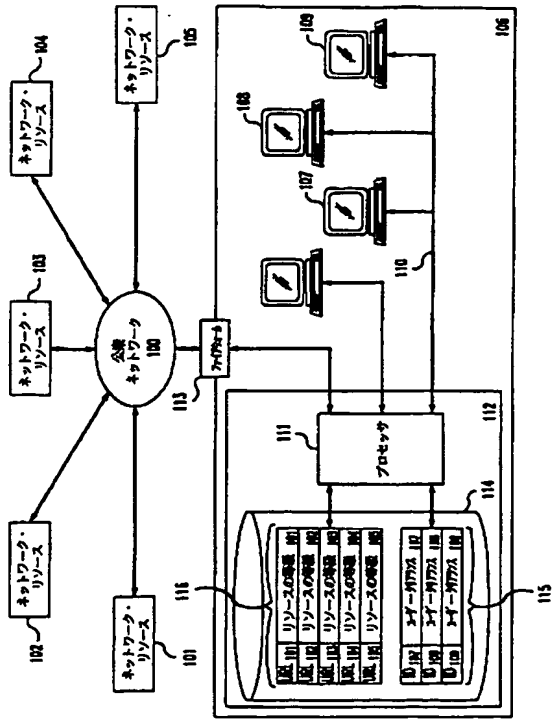
最終頁に続く

(54)【発明の名称】　データベース・アクセス管理のためのシステムと方法

(57)【要約】　（修正有）

【課題】　データベースへのアクセスを選択的に制御する。

【解決手段】　アクセス権を決定するために、使用される関連データベースは、管理者によってアクセス等級情報が容易にアップデート、変更される。この関連データベースの中で、特定のリソースの識別子（ＵＲＬ）は、特定のアクセス等級に関連して分類され、リソースの識別子が、ユーザーが管理者によって特定の許可を与えられたアクセス等級に属する場合にのみ、特定のリソースの要求がローカル・ネットワークから公衆の／管理されないデータベースへのリンクを提供するアクセス・グループに送られるように構成される。例えば、ユーザーのローカル・ネットワークの中の代理サーバーの一部分として実現される。



【特許請求の範囲】

【請求項１】　１つかそれ以上の、それ以外の点では公衆の情報リソースへのアクセスを選択的に制限するためのシステムであって、

複数のリソースの識別子の各々を少なくとも１つのリソースの等級と関連させる第１の記憶されたリストと、複数のユーザー識別コードの各々を少なくとも１つのユーザー・クリアランスの等級と関連させる第２の記憶されたリストとを含む関連データベースと、

リソースの識別子とユーザー識別コードを含む、１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスの要求を受信するために適用され、さらに前記関連データベースの中の第１、第２リストを照会し、前記第１リストの中の前記受信されたリソースの識別子と関連して示されたリソースの等級と、前記第２リストの中の前記受信されたユーザー識別コードと関連して示されたユーザー・クリアランスの等級との相関として、前記１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスの要求を実行するために適用されたプロセッサとを含む、システム。

【請求項２】　前記１つかそれ以上の特定のネットワーク・リソースの少なくとも１つが、少なくとも１つのインライン・イメージを含む、請求項１に記載のシステム。

【請求項３】　前記第１リストの中の前記受信されたリソースの識別子と関連するリソースの等級が、前記第２リストの中の前記受信されたユーザー識別コードと関連する前記ユーザー・クリアランスの等級の少なくとも１つと一致する場合、前記プロセッサが前記アクセスの要求を実行するようにプログラムされる、請求項１に記載のシステム。

【請求項４】　前記第１リストの中の前記受信されたリソースの識別子と関連するリソースの等級が、前記第２リストの中の前記受信されたユーザー識別コードと関連する前記ユーザー・クリアランスの等級の少なくとも１つと一致する場合、前記プロセッサが前記アクセスの要求を拒否するようにプログラムされる、請求項１に記載のシステム。

【請求項５】　前記プロセッサが、ネットワークの代理サーバーの中に含まれる、請求項１に記載のシステム。

【請求項６】　前記ユーザー識別コードの各々が、１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスを促進するために適用される１つかそれ以上のターミナルを識別する、請求項１に記載のシステム。

【請求項７】　前記ユーザー識別コードの各々が、１つかそれ以上の特定のネットワーク・リソースにアクセスすることを許可された１人かそれ以上の個人を識別する、請求項１に記載のシステム。

【請求項８】　前記リソースの識別子の各々が、１つかそれ以上の特定のネットワーク・リソースにアクセスするための１つかそれ以上の共通のリソース・ロケータに一致する、請求項１に記載のシステム。

【請求項９】　前記関連データベースがさらに、前記複数のリソースの識別子の１つかそれ以上と関連するデータ・リストを含み、前記データ・リストが、前記第１リストの中の前記複数のリソースの識別子の前記１つかそれ以上と関連して示されたリソースの等級に関する文書の情報を表す、請求項１に記載のシステム。

【請求項１０】　前記関連データベースがさらに、１つかそれ以上の前記リソースの識別子と関連する条件的なデータ・リストを含み、前記条件的なデータ・リストが、前記リソースの識別子と関連する特定のネットワーク・リソースへのネットワーク・アクセスの要求が実行される詳細な条件を示す情報を表し、前記プロセッサがさらに、前記条件的なデータ・リストの相関として、前記１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスの前記要求を実行するために適用される、請求項１に記載のシステム。

【請求項１１】　前記関連データベースがさらに、少なくとも１つのシステム・マネージャの識別子の記憶されたリストを含み、前記プロセッサが前記システム・マネージャの識別子のリストに基づいて、ユーザーをシステム・マネージャとして識別し、前記識別されたシステム・マネージャに前記関連データベースの内容の変更を許可するために適用される、請求項１に記載のシステム。

【請求項１２】　前記関連データベースがさらに、前記関連データベースの内容の、前記識別されたシステム・マネージャによる変更を促進するために適用される少なくとも１つのＨＴＭＬページを含む、保存されたリストを含む、請求項１１に記載のシステム。

【請求項１３】　１つかそれ以上の、それ以外の点では公衆の情報リソースへのアクセスを選択的に制限するための方法であって、

ユーザー識別コードとリソースの識別子を含む、１つかそれ以上の特定の情報リソースにアクセスするための要求を受信するステップと、

前記リソースの識別子の各々が少なくとも１つのリソースの等級と関連し、前記ユーザー識別コードの各々が少なくとも１つのユーザー・クリアランスの等級と関連する、ユーザー識別コードとリソースの識別子の記憶されたリストを含む関連データベースへのアクセスの前記受信された要求を比較するステップと、

前記記憶されたリストの中の前記受信されたリソースの識別子と関連して示されたリソースの等級と、前記記憶されたリストの中の前記受信されたユーザー識別コードと関連して示されたユーザー・クリアランスの等級の相関としてアクセスの前記要求を実行するステップとを含む、方法。

【請求項１４】　前記１つかそれ以上の特定のネットワ

ーク・リソースの少なくとも１つが少なくとも１つのインライン・イメージを含む、請求項１３に記載の方法。

【請求項１５】　前記記憶されたリストによって、少なくとも１つのユーザー・クリアランスに関連する前記受信されたユーザー識別コードが、前記１つかそれ以上の特定のネットワーク・リソースに関連する少なくとも１つのリソースの等級に一致することが示される場合、前記アクセスの要求が実行される、請求項１３に記載の方法。

【請求項１６】　前記記憶されたリストによって、少なくとも１つのユーザー・クリアランスに関連する前記受信されたユーザー識別コードが、前記１つかそれ以上の特定のネットワーク・リソースに関連する少なくとも１つのリソースの等級に一致することが示される場合、前記アクセスの要求が拒否される、請求項１３に記載の方法。

【請求項１７】　前記ユーザー識別コードの各々が、１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスを促進するために適用される１つかそれ以上のターミナルを識別する、請求項１３に記載の方法。

【請求項１８】　前記ユーザー識別コードの各々が、１つかそれ以上の特定のネットワーク・リソースへのアクセスを許可された１人かそれ以上の個人を識別する、請求項１３に記載の方法。

【請求項１９】　前記リソースの識別子の各々が、前記１つかそれ以上の特定のネットワーク・リソースにアクセスするための１つかそれ以上の共通のリソース・ロケータに一致する、請求項１３に記載の方法。

【請求項２０】　ユーザーに前記関連データベースの中のデータ・リストへのアクセスを供給し、前記データ・リストが前記複数のリソースの識別子の１つかそれ以上と関連しており、前記データ・リストが前記記憶されたリストの中の前記複数のリソースの識別子の前記１つかそれ以上と関連して示される、リソースの等級に関する文書の情報を表す、ステップをさらに含む、請求項１３に記載の方法。

【請求項２１】　前記関連データベースがさらに、少なくとも１つのシステム・マネージャの識別子の記憶されたリストを含み、前記プロセッサが、前記システム・マネージャの識別子のリストに基づいて、ユーザーをシステム・マネージャとして識別し、前記識別されたシステム・マネージャに前記関連データベースの内容変更を許可するために適用される、請求項２２のステップをさらに含む、請求項１３に記載の方法。

【請求項２２】　１つかそれ以上の、それ以外の点では公衆の情報リソースへのアクセスを選択的に制限するためのシステムであって、

複数のリソースの識別子を少なくとも１つのリソースの等級と関連させる第１の記憶されたリストと、複数のユーザー識別コードを少なくとも１つのユーザー・クリアランスの等級と関連させる第２の記憶されたリストを含む関連データベースと、

要求がリソースの識別子とユーザー識別コードを含み、プロセッサが前記関連データベースの中の前記第１、第２リストに照会し、前記第１リストの中の前記受信されたリソースの識別子と関連して示されるリソースの等級と、前記第２リストの中の前記受信されたユーザー識別コードと関連して示されるユーザー・クリアランスの相関として、前記１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスを実行するために適用される、１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスの要求を受信するために提供されるプロセッサとを含む、システム。

【請求項２３】　前記１つかそれ以上の特定のネットワーク・リソースの少なくとも１つが、少なくとも１つのインライン・イメージを含む、請求項２２に記載のシステム。

【請求項２４】　少なくとも１つのリソースの等級と関連する前記複数のリソースの識別子が階層ディレクトリ・データ構造で配置される、請求項２２に記載のシステム。

【請求項２５】　前記階層ディレクトリ・データ構造で配置された前記複数のリソースの識別子が、１つ以上のリソースの等級と関連する、請求項２４に記載のシステム。

【請求項２６】　前記第１ストの中の前記受信されたリソースの識別子と関連する前記リソースの等級が、前記第２リストの中の前記受信されたユーザー識別コードと関連する前記ユーザー・クリアランスの等級の少なくとも１つに一致する場合、前記プロセッサが前記アクセスの要求を実行するようにプログラムされる、請求項２２に記載のシステム。

【請求項２７】　前記第１リストの中の前記受信されたリソースの識別子と関連する前記リソースの等級が、前記第２リストの中の前記受信されたユーザー識別コードと関連する前記ユーザー・クリアランスの等級の少なくとも１つに一致する場合、前記プロセッサが前記アクセスの要求を実行を拒否するようにプログラムされる、請求項２２に記載のシステム。

【請求項２８】　前記プロセッサがネットワーク代理サーバーの中に含まれる、請求項２２に記載のシステム。

【請求項２９】　前記ユーザー識別コードの各々が、１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスを促進するために適用される、１つかそれ以上のターミナルを識別する、請求項２２に記載のシステム。

【請求項３０】　前記ユーザー識別コードの各々が、１つかそれ以上の特定のネットワーク・リソースへのアクセスを許可された１人かそれ以上の個人を識別する、請

求項２２に記載のシステム。
【請求項３１】　前記リソースの識別子の各々が、１つかそれ以上の特定のネットワーク・リソースにアクセスするための１つかそれ以上の共通のリソース・ロケータに一致する、請求項２２に記載のシステム。
【請求項３２】　前記関連データベースがさらに、前記複数のリソースの識別子の１つかそれ以上と関連するデータ・リストを含み、前記データ・リストが、前記第１リストの中の前記複数のリソースの識別子の前記１つかそれ以上と関連して示される、リソースの等級に関する文書の情報を表す、請求項２２に記載のシステム。
【請求項３３】　前記関連データベースがさらに、１つかそれ以上の前記リソースの識別子と関連する条件的なデータ・リストを含み、前記条件的なデータ・リストが、前記リソースの識別子に関連する特定のネットワーク・リソースへのネットワーク・アクセスの要求が実行される特定の条件を示す情報を表し、前記プロセッサがさらに、前記条件的なデータ・リストの相関として、前記１つかそれ以上の特定のネットワーク・リソースへのネットワーク・アクセスの前記要求を実行するために適用される、請求項２２に記載のシステム。
【請求項３４】　前記関連データベースがさらに、少なくとも１つのシステム・マネージャの識別子の記憶されたリストを含み、前記プロセッサが、前記システム・マネージャの識別子のリストに基づいて、ユーザーをシステム・マネージャとして識別し、前記識別されたシステム・マネージャに前記関連データベースの内容変更を許可するために適用される、請求項２２に記載の方法。
【請求項３５】　前記関連データベースがさらに、前記関連データベースの内容の、前記識別されたシステム・マネージャによる変更を促進するために適用される少なくとも１つのＨＴＭＬページを含む、保存されたリストを含む、請求項３４に記載のシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データベース・アクセスの制御に関し、より詳細には、それ以外の点では公衆のデータベースに関して選択的にこの種の制御を提供することに関する。
【０００２】
【関連出願に対する相互参照】本出願は、「データベース・アクセス管理のためのシステムと方法」と題された、１９９５年６月６日出願の、米国特許出願第０８／４６９、２７６号の一部継続出願である。
【０００３】
【従来の技術】世界中のコンピュータのファイルまたは他のリソースは、インターネットとして知られるネットワークの集積を通じて他のコンピュータのユーザーに、公に利用可能になる。ハイパーテキスト・マークアップ・ランゲージ（「ＨＴＭＬ」）で書かれたファイルを使って結合された公に利用可能な全てのリソースの集合は、ワールド・ワイド・ウェブ（「WWW」）として知られている。
【０００４】インターネットに接続されたコンピュータのユーザーは、クライアントとして知られる、WWWの一部であるリソースを要求するプログラムを始動する。するとサーバー・プログラムが要求を処理し、指定されたリソースを（それが現在利用可能なものならば）送り返す。ユニフォーム・リソース・ロケーター（「ＵＲＬ」）として知られる標準命名規定が適用されてきた。この規定は、現在、ハイパーテキスト・トランスポート・プロトコル（「ｈｔｔｐ」）、ファイル・トランスポート・プロトコル（「ｆｔｐ」）、ｇｏｐｈｅｒ、ワイド・エリア・インフォメーション・サービス（「ＷＡＩＳ」）といった下位区分を含む、多くのタイプのロケーション名を含んでいる。リソースは、ダウンロードされる時、追加リソースのＵＲＬを含むことがある。従って、クライアントのユーザーは、容易に自分が特に要求していない新しいリソースの存在を知ることが出来る。
【０００５】WWWを通じてアクセス可能な様々なリソースが、世界中のコンピュータに関わる多くのいろいろな人々によって、内容を集中的に管理されることなく製作、維持されている。この管理されない情報のコレクションに含まれる情報や映像の種類によっては、ある種のユーザーにふさわしくないものがあるので、WWWリソースへのアクセスを選択的に制限出来ることが望ましい。例えば、両親や学校の教師は、子供が有益な情報にアクセスすることを望むが、猥褻な資料（子供がWWWを知らずに探査した結果、または偶然のＵＲＬのダウンロードを通じてさらされる）へのアクセスは望まない。別の例は、クラスのミーティングの間、生徒に特定のグループのリソースにだけアクセスさせたいと思う学校の教師の場合である。第３の例は、従業員に、仕事関係のリソースにだけアクセスして、WWWの探査で時間を浪費しないようにして欲しいと思う経営者である。一般に、異なった科目の授業の間、生徒が異なったリソースの組み合わせに制限される場合のように、特定のユーザーは異なった時間に異なったリソースに制限される必要がある。
【０００６】学校のような機関によっては、ユーザーに、例えば、猥褻な資料をダウンロードしないといった、WWWの探査を制限することに同意する申し立てに従うことを要求することもある。
【０００７】
【発明が解決しようとする課題】しかし、こうした方針に自発的に従っても、ダウンロードしたり見たりする前に禁止されているかまたは不適当であると容易に識別出来ないリソースの偶発的なダウンロードは防止出来ない。
【０００８】「ファイアウォール」と呼ばれる技術的な

解決法も、WWWとインターネットへのアクセスを制限または妨害するために当然利用可能である。ファイアウォールは、普通、ローカル・エリア・ネットワーク（「ＬＡＮ」）のコンピュータを部外者の攻撃から守るために設置されるソフトウェアによるゲートウェイである。ファイアウォールを設置する効果の１つは、WWWのクライアントが直接WWWのサーバーにコンタクト出来なくなることである。通常、これは余りに制限的であり、ユーザーはWWWのクライアントによって直接コンタクトされる「代理サーバー」の力を借りる。代理サーバーには、ファイアウォールを通じて要求を送り、これにより、サーバーとのインターネットでの通信を提供する特殊な能力がある。効率を上げるために、代理サーバーはあるリソースを局所的にキャッシュすることもある。使用中のクライアントと代理サーバーは、WWWの全ての公衆リソースへのアクセスを生じる。それらは特定のユーザーにある種のリソースを要求することを許可し、同じユーザーが他のリソースにアクセスすることを禁止するように構成されていない。

【０００９】利用可能なWWWリソースのある種の「フィルタリング」が、間接的アクセスを提供するシステム内で行われることもある。こうしたシステムでは、情報プロバイダがリソースをWWWからダウンロードし、リソースのコピーを維持する。ユーザーはそのコピーにアクセスする。情報プロバイダはWWWからリソースを得る際それを検討し、ユーザーに利用出来るようにする前に不適当または猥褻な部分を編集して取り除く。このスキームの欠点は、情報プロバイダによって供給される資料がWWW上の元のリソースに比べて古いものになってしまう点である。

【００１０】WWWのリソースへの「フィルタリングされた」アクセスの別のスキームでは、代理サーバーがユーザーにアクセスが許可されているリソースのメニューを供給し、ユーザーは、メニューのリソースからの一連のリンクによって到達出来る任意のリソースを得ることが出来る。ユーザーはこのメニュー経由でのみＵＲＬの要求が許可される。この方法には２つの欠点がある。第１に、多くのリソースが、それ自体は受け入れられるものであっても、不適当な資料へのリンクを含むために除外されなければならない。第２に、リソースが時間と共に変更されて不適当な資料に導く新しいリンクを含むようになり、ユーザーにそうした不適当な資料にアクセスする故意でない道を提供することがある。

【００１１】WWWのリソースへの「フィルタリングされた」アクセスのさらに他の方法では、クライアントまたは代理サーバーが、許可されない単語（すなわち、猥褻な言葉、性的用語等）のリストによって各リソースをチェックし、ユーザーにこうした単語を含まないリソースだけを示す。しかし、この方法では映像のフィルタリングが出来ないし、特定の単語以外の内容によって不適当なリソースを禁止することも出来ない。

【００１２】ユーザーを不適当または猥褻な資料から守るさらに他の手段が、コンピュータ、ビデオ・ゲームのメーカーによって確立された。ゲームは、暴力、裸体／セックス、言語の次元によって自主的に等級付けされる。こうした規定はまだWWWでは適用されていないが、類似のものが、恐らくは偽造を防止するためのデジタル・シグネチャと共にWWWのリソースの等級付けを行う。するとWWWのクライアントは、そのようにプログラムされれば、等級付けされていないか、ある利用者に取って受け入れられない等級のリソースをセーブまたはディスプレイしないように選ぶことが出来る。このスキームの欠点は、有益なサーバーを提供する多くの人々（非職業的または無償でやっている人も多い）を、等級リストに従うよう説得する必要があることである。

【００１３】WWWで利用出来る、管理されない公衆データベース・リソースへのユーザーのアクセスを制限するための既存のシステムは全て、明らかな欠点を持っている。現在、権威者（すなわち、教師、監督者、システム管理者等）にとって、１人かそれ以上のユーザーによるWWWへのアクセスを、そのユーザーのインターネットとの通信能力を大きく損なうことなく、選択的に制御する容易な手段は存在しない。これは、こうした制御を行いたいと望む権威者が、情報／サービス・ネットワークの運営に関してコンピュータに余り熟練していない場合、特にそうである。

【００１４】

【課題を解決するための手段】本発明は、１人かそれ以上のネットワーク管理者／マネージャが特定の情報またはサービスを等級付け出来るようにするシステムと方法を提供することによって、ネットワーク・データベースへのアクセスを調整するための従来のスキームの欠陥を克服する。この等級は、特定のシステム・ユーザーがある公衆または管理されないデータベース（すなわち、WWWとインターネット）経由で情報／サービスにアクセスすることを制限するために使われる。本発明は、アクセス権を決定し、等級情報を記憶するために、関連データベースを使用する。等級情報データベースは、管理者／マネージャによって容易にアップデート、変更される。この関連データベースの中には、特定のリソースの識別子（すなわち、ＵＲＬ）が特定のアクセスの等級と関連されて分類される。関連データベースは、システムの各ユーザーにとって、リソースの識別子が、管理者／マネージャによってユーザーに明確な許可を与えられたアクセスの等級を持つ場合にのみ、特定のリソースへの要求が、ローカル・ネットワークから、公衆の／管理されないデータベースへのリンクを提供するサーバーに通るように配置される。１つの好適な実施例では、本発明は、ユーザーのローカル・ネットワークの中の代理サーバーの一部分として実現される。他の実施例では、シス

テムは、特定のリソースの識別子の各々と関連する等級リソース・ファイルを維持し、特定のリソースに関するコメント、条件等が記憶される。

【００１５】

【発明の実施の形態】図１は、本発明の実施例のシステムの単純化したダイアグラムである。関連するシステムは、１９９５年６月６日出願の、「データベース・アクセス制御のためのシステムと方法」と題された、同時係属出願の、共通に譲渡された米国特許出願第０８／４６９、３４２号の主題である。図１に示すように、本システムには、公衆ネットワーク１００、ネットワーク・リソース１０１～１０５、ユーザー・サイト１０６が含まれる。ユーザー・サイト１０６の特定のユーザーはユーザー・ターミナル１０７、１０８、１０９を経由して公衆ネットワーク１００へのアクセスを得る。こうしたユーザー・ターミナルの各々は、ローカル・エリア・ネットワーク（「ＬＡＮ」）１１０によって代理サーバー１１２内のプロセッサ１１１にリンクされている。最後に、代理サーバー１１２は、ファイアウォール１１３経由でプロセッサ１１１から公衆ネットワーク１００への接続を提供する。

【００１６】公衆ネットワーク１００を通じてネットワーク・リソース（１０１～１０５）にアクセスするための、ユーザー・ターミナル１０７～１０９からの要求は、代理サーバー１１２内のプロセッサ１１１に送られる。本発明のこの特定の実施例では、送られた要求はＵＲＬの形を取っていると考えられる。技術上良く知られているように、ＵＲＬが代理サーバーに送られる時、要求を出している特定のユーザー・ターミナルは、ＵＲＬに付けられた識別ヘッダによって代理サーバーに識別される。図１に示すシステムでは、ユーザー・ターミナル１０７のための識別コードはID_{107}、ユーザー・ターミナル１０８のための識別コードはID_{108}、ユーザー・ターミナル１０９のための識別コードはID_{109}である。さらに、図１のシステムの中では、URL_{101}、URL_{102}、URL_{103}、URL_{104}、URL_{105}はそれぞれ、ネットワーク・リソース１０１、１０２、１０３、１０４、１０５からの情報の要求を示す。

【００１７】入ってくるＵＲＬを受信すると、プロセッサ１１１はＵＲＬヘッダから要求するユーザー・ターミナルを識別するようプログラムされる。この識別情報は、プロセッサ１１１によって、受信したＵＲＬを関連データベース１１４に記憶された情報と相互参照するために利用される。関連データベース１１４は、各ユーザー識別コード（ID_{107}、ID_{108}、ID_{109}）をユーザー・クリアランス・コード（それぞれ、ユーザー・クリアランス１０７、ユーザー・クリアランス１０８、ユーザー・クリアランス１０９）と関連させるリスト１１５を含む。これらのユーザー・クリアランスは、あるユーザー・ターミナルがアクセスを許可されるネットワーク・リソースの特定の等級のクラス（すなわち、無制限のアクセス、暴力的な内容にアクセスするよう識別されたＵＲＬの制限的使用、猥褻な内容にアクセスするよう識別されたＵＲＬの制限的使用等）を示す。関連データベース１１４には、ネットワーク・リソースにアクセスするためにユーザー・ターミナルからの伝送を許容されるＵＲＬ（URL_{101}～$_{105}$）のレジスタを含むリスト１１６も含まれる。リスト１１６は各ＵＲＬを特定のリソース等級データ（リソースの等級$_{101}$～$_{105}$）と関連させる。前記ＵＲＬの各々と関連するリソースの等級は、等級クラスのインジケータと同じように単純なものでよい。例えば、ある特定のＵＲＬが、全てのユーザーの使用を認められているか、またはある特定のＵＲＬの使用が何らかの理由で制限されていること（すなわち、暴力的または猥褻な内容を含むネットワーク・リソースにアクセスするＵＲＬ）の表示である。

【００１８】例えば、システム管理者またはマネージャが図１のネットワーク・リソースを３つのクラス（非暴力的－ＮＶ、やや暴力的－ＭＶ、暴力的－Ｖ）に、次のように主観的に分類したと仮定する。ネットワーク・リソース１０１－ＮＶ、ネットワーク・リソース１０２－ＮＶ、ネットワーク・リソース１０３－ＮＶ、ネットワーク・リソース１０４－ＭＶ、ネットワーク・リソース１０５－Ｖ。この時ＵＲＬ／リソースの等級のリスト１１６は次のデータを含む。

【表１】

URL	リソースの等級
URL_{101}	NV
URL_{102}	NV
URL_{103}	NV
URL_{104}	MV
URL_{105}	V

【００１９】さらに、ユーザー・ターミナル１０７は全てのネットワーク・リソース（ＮＶ、ＭＶ、Ｖ）へのアクセスを認められ、ユーザー・ターミナル１０８はＮＶ、ＭＶと等級付けされたリソースへのアクセスのみ認められ、ユーザー・ターミナル１０９はＮＶリソースへのアクセスのみ認められると仮定する。こうしたユーザー・ターミナルのクリアランスを反映した情報がリスト１１５の中に次のように記憶される。

【表２】

ユーザーの識別コード	ユーザーのクリアランス
ID_{107}	NV, MV, V
ID_{108}	NV, MV
ID_{109}	NV

【００２０】図１のシステムの中で、要求するユーザー・ターミナルがＵＲＬをＬＡＮ１１０経由送信する時、プロセッサ１１１はＵＲＬと要求するユーザー・ターミナルの識別コードを受信する。するとプロセッサ１１１はその特定の要求するユーザー・ターミナルのために認められているリソースを判断するためにリスト１１５を照会し、特定の受信されたＵＲＬによってアクセスされるネットワーク・リソースのリソースの等級を判断するためにリスト１１６を照会する。ネットワーク・リソース１０１を要求するＵＲＬがプロセッサ１１１によってユーザー・ターミナル１０７から受信された場合、関連データベース１１４の中のリスト１１５、１１６は、ユーザー・ターミナル１０７がＮＶ、ＭＶ、Ｖ等級のネットワーク・リソースへのアクセスを許可されており、URL_{101} がＮＶ等級であるという情報をもたらす。要求されたリソースの等級が要求したユーザー・ターミナルにとって許可されているものの１つだったので、プロセッサ１１１は情報（URL_{101} ）への要求をファイアウォール１１３を経由して公衆ネットワーク１００に送る。要求されたリソースが利用可能であれば、公衆ネットワークは要求された情報をファイアウォール１１３、プロセッサ１１１、ＬＡＮ１１０経由ユーザー・ターミナル１０７に返す。反対に、要求するユーザー・ターミナルが許可されていない等級を持つＵＲＬが受信された場合、情報への要求は拒否される。例えば、URL_{105} がプロセッサ１１１によってユーザー・ターミナル１０９から受信された場合、関連データベース１１４がアクセスされる。リスト１１５、１１６のデータが、URL_{105} はＶの等級を持っており、ユーザー・ターミナル１０９はＮＶ等級のネットワーク・リソースへのアクセスしか許可されていないことを示すので、プロセッサ１１１は情報の要求を拒否し、ＵＲＬは公共ネットワーク１００に送られない。プロセッサ１１１は、ユーザー・ターミナルからの等級付けされていない情報の要求を全て拒否するようにもプログラム出来る。このことによって、システム管理者／マネージャによって検討または等級付けされていないネットワーク・リソースへのアクセスが禁止される。本発明の上記の説明から、あるリソースの中に含まれる映像（すなわち、インライン・イメージ）がリソースに与えられるのと同じ等級の対象になることも理解される。インライン・イメージを別に等級付けする必要はない。

【００２１】上記で説明した特定の実施例では、関連データベース１１４は、各ユーザー・ターミナルが公衆ネットワーク１００から検索することを許可されたネットワーク・リソースの等級付けを反映したユーザー・ターミナル識別コードと様々なユーザー・クリアランスを記憶する。本発明は、あるユーザー・ターミナル識別コードと関連するユーザー・クリアランスのリストが制限リスト（すなわち、ユーザーはその等級を持つネットワーク・リソースの検索を許可されない）として働くように変更出来ることが理解される。この制限リスト機能はプロセッサ１１１の再プログラミングによって容易に促進される。さらに、本発明は、プロセッサ１１１によって認識され関連データベース１１４に記憶される識別コードが、ユーザー・ターミナル固有のものでなく、ユーザー固有のものであるように変更出来る。別言すると、図１のシステムは、ターミナルを使うある個人がシステムに対して個人のパスワードなどの識別コードによって識別されるように変更出来る。特定のＵＲＬの伝送のアクセスまたは拒否が、システムによって、個人が利用する特定のユーザー・ターミナルとは無関係に、個人の識別コードの相関として行われる。

【００２２】上記で説明したシステムは、ＵＲＬが、関連データベースのメモリ構造の中の等級カテゴリーの中にあるものとして識別されるようにも変更出来る。図２は、図１と同様だが、ＵＲＬの等級グループへの分類を促進するよう適用されたシステムの単純化したダイアグラムを提供する。図示されるように、関連データベース２００はユーザー識別コードのリスト２０１とＵＲＬのリスト２０２を含む。リスト２０１は、ユーザー識別コードID_{107} 、ID_{108} をユーザー・クリアランスＡカテゴリーにあるものとし、またID_{109} をユーザー・クリアランスＢカテゴリーにあるものとする。入ってきたＵＲＬを受信すると、プロセッサ１１１はＵＲＬヘッダから要求するユーザー・ターミナルの識別コードを確認し、この識別情報を利用してリスト２０１の中でその特定のユーザーのために指定されたクリアランス・カテゴリーを判断する。ついで、プロセッサ１１１によって受信された特定のＵＲＬがリスト２０２と相互参照され、関連するリソースの等級カテゴリーが判断される。要求するユーザーが要求されたＵＲＬと関連するリソースの等級に対応するクリアランスを持っている場合、プロセッサ１１１はＵＲＬをファイアウォール１１３経由で公衆ネットワーク１００に送る。公衆ネットワーク１００は要求された情報をファイアウォール１１３、プロセッサ１１１、ＬＡＮ１１０経由で識別されたユーザーに返す。反対に、ＵＲＬが、要求したユーザーが許可されていない等級カテゴリーのリソースに含まれる場合、プロセッサ１１１は情報の要求を拒否する。

【００２３】さらに、上記で説明したシステムの中のＵＲＬ等級データには、ある等級の基礎となる原理のテキ

ストのリスト、またはより複雑に条件付けられた等級付けスキームを促進する追加情報を含む。ＵＲＬの条件付けられた等級の説明として、特定のＵＲＬに関連するリソースの等級が、暴力的であることを示すＶと等級付けされ、ある学校の中のターミナルは全てＮＶ（非暴力的）のクリアランスを持つと仮定する。従って、一般に、その学校のターミナルはＶ等級のＵＲＬの使用を承認されない。しかし、この一般的なルールの例外が必要となる状況が起こり得る。例えば、歴史の授業に関連するあるターミナルが、暴力的であるが、歴史的な軍事戦闘に関する情報を含むリソースにアクセスする必要を生じることがある。こうしたリソースへのアクセスを促進するために、軍事戦闘に関するリソースの関連データベース等級情報は、「歴史の教室にあるユーザー・ターミナルについてはＮＶ、他の全てのターミナルについてはＶ」という条件的な等級を反映するように拡大される。この条件付けシステムによって、歴史の教室のターミナルは、他の全ての「暴力的」と等級付けされたＵＲＬから制限されるが、暴力的だが、歴史的に重要なネットワーク・リソースにアクセスすることが出来る。条件付けられたアクセスは、時間との相関によってもターミナルまたはユーザーに対して承認される（すなわち、アクセスが１日のある時間あるユーザーまたはユーザー・ターミナルに対して制限される）。

【００２４】上記のように、図１、図２のシステムの中の関連データベースはユーザー／ユーザー・ターミナルの識別コードとＵＲＬのリストを含む。これらのリストは、それ以外の点では公衆のネットワーク・リソースの選択的アクセスを促進するために、主観的に分類または等級付けされる。この分類／等級付けは、システム・マネージャによって行われるものとされ、本発明を実行する際に利用される関連データベースの内容を変更することによって達成される。図３のシステムの中で、プロセッサ１１１は、関連データベース３０２の中のリソース分類情報（リスト３００）および／またはユーザー／ユーザー・ターミナル・クリアランス情報（リスト３０１）が、特定の専用マネージメント・ターミナル３０３によってのみ変更出来るようにプログラム出来る。マネージメント・ターミナル３０３が関連データベース３０２に新しい情報を「書き込み」する能力を制限することで、データベースを歪曲する機会は最少になる。また、本システムは、データベースの変更がユーザー・ターミナル１０７、１０８、１０９のどれからでも行えるようにも構成出来る。関連データベース３０２の内容の改悪を防止するために、ユーザー・ターミナルから関連データベース３０２の内容を変更する権限付与が、マネージャの識別子を使って管理される。例えば、システム・マネージャが関連データベース３０２をユーザー・ターミナル１０８から変更したい場合、彼または彼女は自分が権限のあるシステム・マネージャであることを証明するパスワードを入力する。パスワードはプロセッサ１１１によって受信され、マネージャＩＤメモリ・リスト３０４の内容と比較される。受信されたマネージャＩＤパスワードがリスト３０４に記憶されたものと一致する場合、ユーザー・ターミナル１０８は、（リスト３０４に記憶されたＩＤ$_{108}$ によって示されるので）マネージャ・ターミナルとして認められる。その後関連データベース３０２の内容の変更はこのユーザー・ターミナルから行われる。全ての変更が完了すると、マネージャはログオフし、ユーザー・ターミナル１０８は普通のユーザー・ターミナルの状態に戻る（すなわち、ＩＤ$_{108}$ はリスト３０４から消去される）。

【００２５】家庭、学校、職場の環境で情報システムがますます増加するのに伴って、情報のアクセスを管理する責任が、コンピュータまたは情報システムに関して余り熟練していない１人かそれ以上の個人にかかることが多くなっている。上記で説明したシステムは全て、非熟練者のマネージャが容易にシステムを管理出来るような方法で実現出来る。例えば、図３のシステムの中で、プロセッサ１１１は、システム・マネージャとして認識されたユーザーに、各検索されたネットワーク・リソースのリード・ページの前に、ＨＴＭＬ「等級付けヘッダ」を供給するようプログラム出来る。マネージャが公衆ネットワーク１００経由でＡＴ＆Ｔ８００ディレクトリを検索した場合、帰ってきた情報は、プロセッサ１１１によって非暴力的という等級を反映して表示される（図４参照。検索されたリソース、すなわちＡＴ＆Ｔ８００ディレクトリに先行する「ＮＶ」の表示に注意されたい）。マネージャはＨＴＭＬ等級付けページの「ここをクリックして下さい」と表示された部分をクリックすることによって、等級付けの理由を検討出来る。こうすることで、ＮＶという等級の基礎となる理由のリソース分類情報リスト３００を検索することになる（図５に示すページ参照）。マネージャは、ＡＴ＆Ｔ８００ディレクトリ・リソースを検索する際、定められた等級に同意したくない場合、「同意しない場合、ここをクリックして下さい」というところをクリックする。すると、リソース分類情報リスト３００から等級とその理由の情報が検索され、マネージャに等級の編集を行うページを供給する（図６参照）。このページはマネージャにリソースの現在の等級（「ＮＶ」）、そのように等級付けされた主な理由（「暴力的な内容がない」）、より詳細な理由に入るための領域（「本リソースは電話番号リストからなり・・・」）を提供する。ＨＴＭＬページを終了するか変更すると、システム・マネージャは「メッセージの送信」を選択し、ページをリスト３００に記憶するために関連データベース３０２に送信する。

【００２６】上記で説明された特定のシステムと方法は、あくまで本発明の原理を説明するためのものであって、本技術に熟練した者によって、以下の請求項によっ

てのみ制限される本発明の範囲と精神から離れることなく、様々な変更が行われることが理解される。例えば、上記で説明した実施例はいずれも、ユーザー／ユーザー・ターミナルからの、ＵＲＬ以外のフォーマットの要求を受け入れるように変更出来る。関連データベースは、使用され、特定のユーザーのクラスと関連する要求のフォーマットのタイプを示す情報の組み合わせを記憶するように変更するだけでよい。他の変更例としては多マネージャ環境への適応がある。こうした環境では、ネットワーク・リソースの等級は、多数のシステム・マネージャの投票の結果としてもたらされる。例えば、多数のマネージャがリソースの等級を送信したり変更したり出来るが、関連データベースに記憶される最終的な等級は、送信された等級の平均か、マネージャの大多数がそのリソースの等級として選んだものである。本発明を促進するシステムで利用される関連データベースは、許可されるリソースのアクセスを示す情報が、（階層ディレクトリ構造のような）木構造フォーマットで構成されたリソースに適合するように配置されるように構成することも出来る。こうした関連データベースには、特定のリソースの等級と共に表示されるディレクトリまたはサブディレクトリのリストが含まれる。システムは、表示されたディレクトリまたはサブディレクトリの中に位置するリソースが、ディレクトリ／サブディレクトリ全体の等級を引き受けるように構成出来る。または、システムは優先順位ディレクトリ／サブディレクトリ等級付けシステムを利用することも出来る。こうしたシステムでは、ディレクトリは「ＮＶ」といった全体的な等級を与えられる。このＮＶと等級付けされたディレクトリの中の特定のアイテムまたはサブディレクトリは、「Ｖ」の様な、「ＮＶ」以外の特定の等級を付けて分類することが出来る。ユーザーがＮＶ等級のディレクトリにアクセスする時、他の、より詳細な、異なった等級を付けて分類されたアイテムまたはサブディレクトリ以外は、その中の全てのアイテムはＮＶ等級を持つものと考えられる。

【図面の簡単な説明】

【図１】本発明の実施例のシステムの略図である。

【図２】ＵＲＬの等級付けされたグループへの分類を促進するために適用される、図１のシステムの他の構成の略図である。

【図３】システム管理の適用を含む、図１のシステムの他の構成の略図である。

【図４】特定のネットワーク・リソースを検索する際、システム・マネージャに送り返される等級情報の図である。

【図５】ネットワーク・マネージャに提供されるリソース分類情報の図である。

【図６】ネットワーク・マネージャがアクセス出来る等級編集ページの図である。

【符号の説明】

１００　公衆ネットワーク

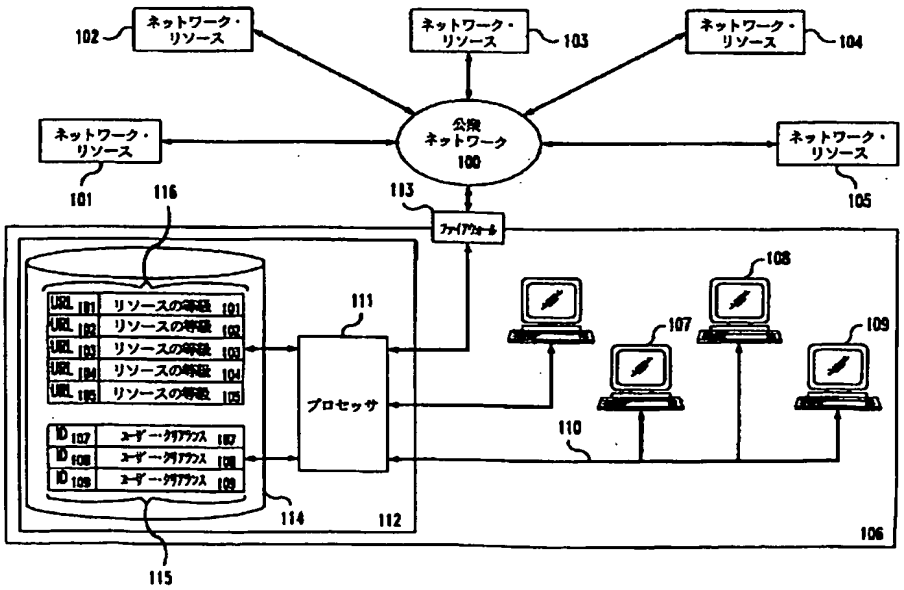
１０１、１０２、１０３、１０４、１０５　ネットワークリソース

１１１　プロセッサ

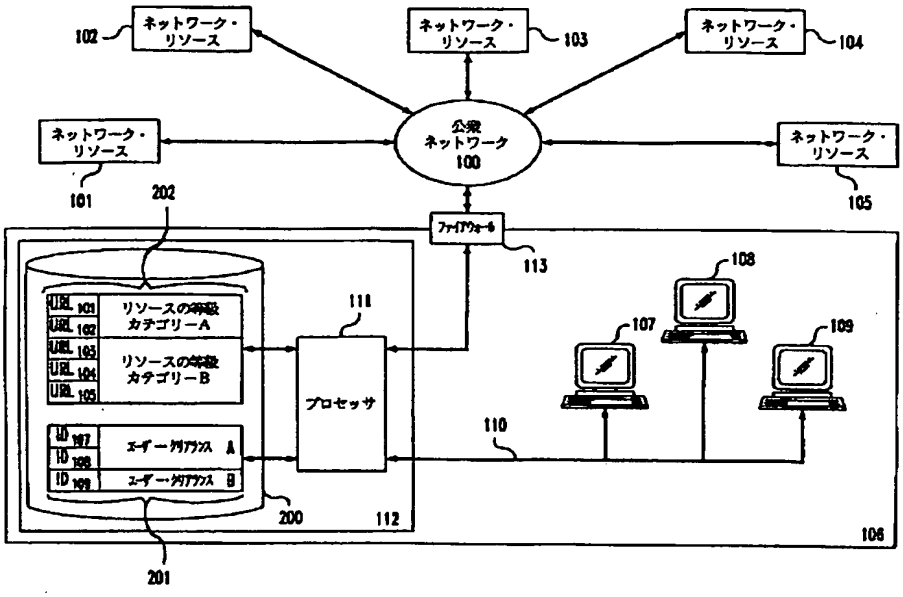
１１５　ユーザー・クリアランス

１１６　リソースの等級

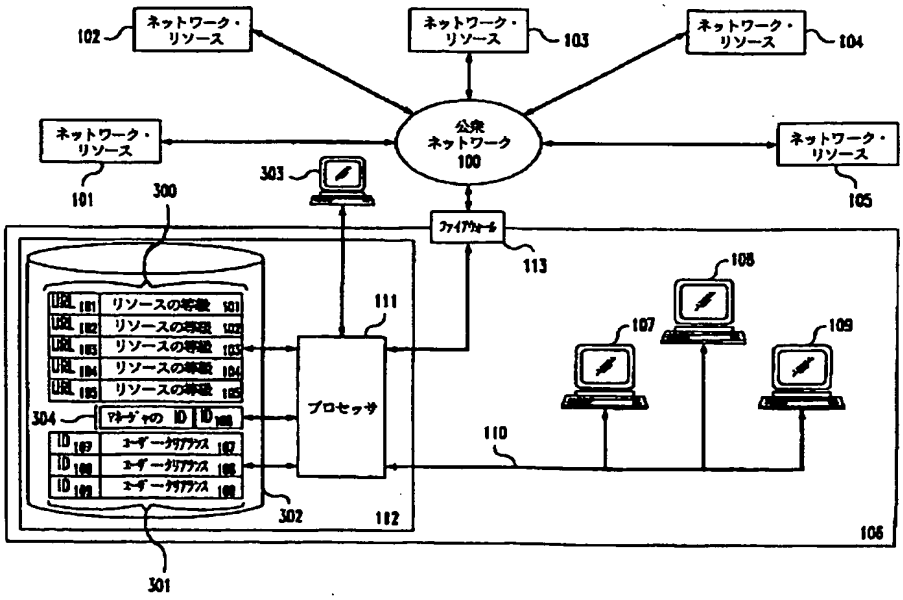
【図１】



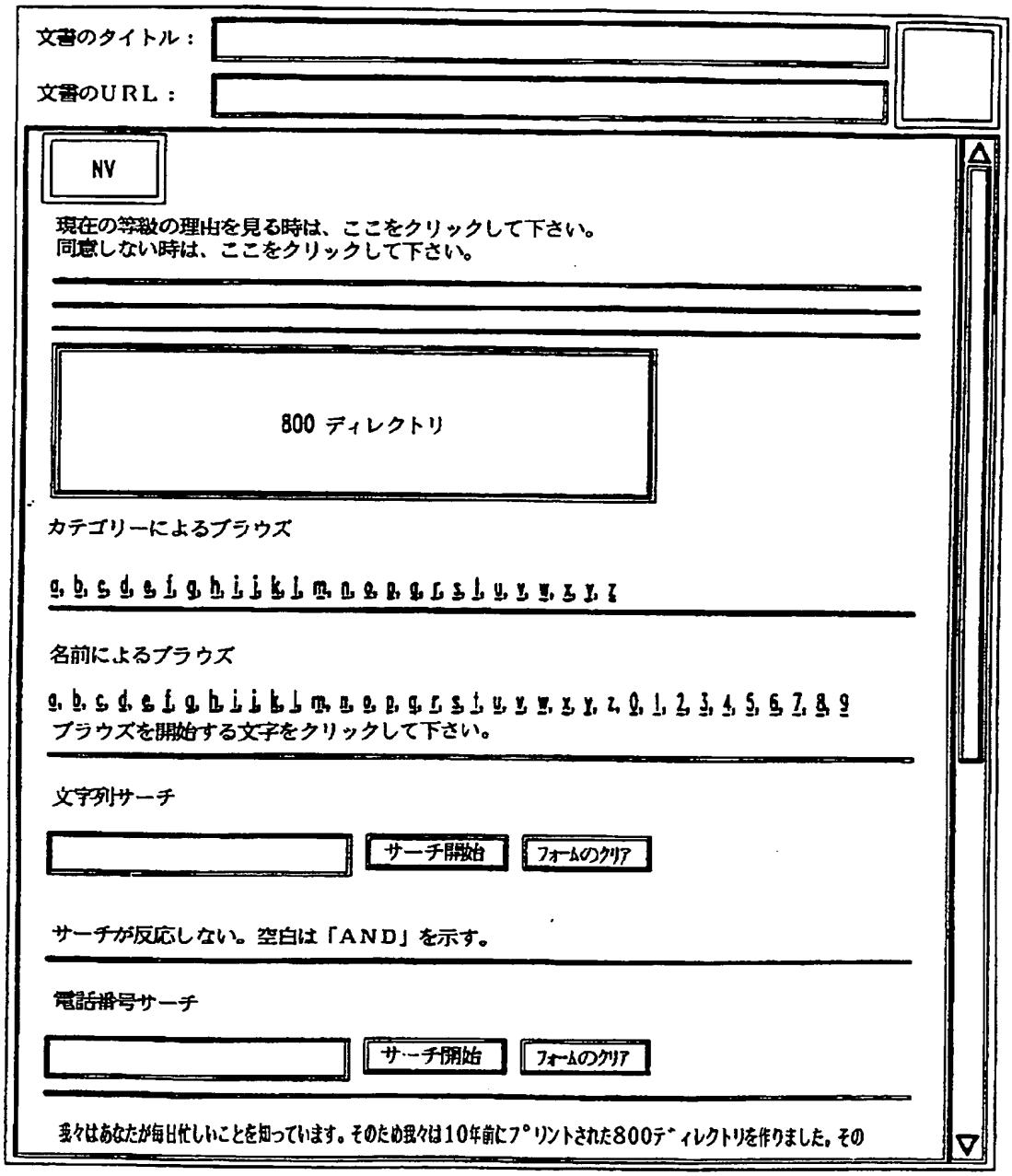
【図２】


102
ネットワーク・リソース
103
104
公衆ネットワーク 100
101
105
202
113
108
107
109
111
リソースの等級 カテゴリーA
リソースの等級 カテゴリーB
プロセッサ
110
200
112
106
201

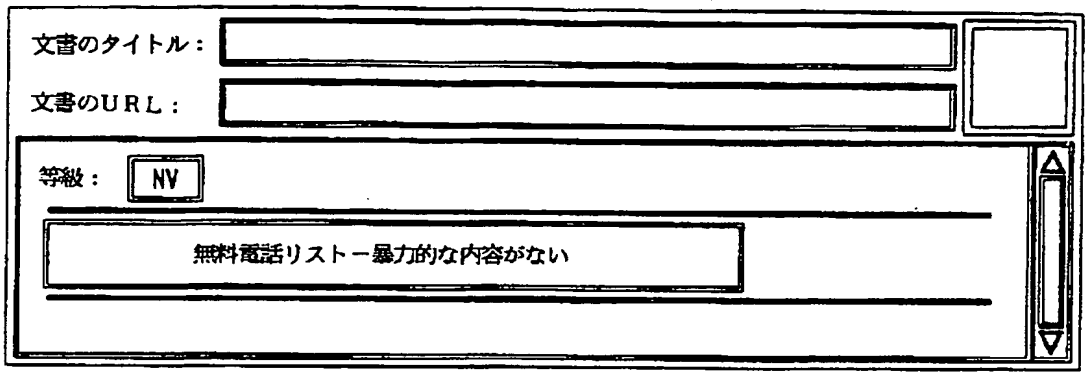
【図３】


102
ネットワーク・リソース
103
104
公衆ネットワーク 100
101
105
303
300
113
108
107
109
111
プロセッサ
304
110
302
112
106
301

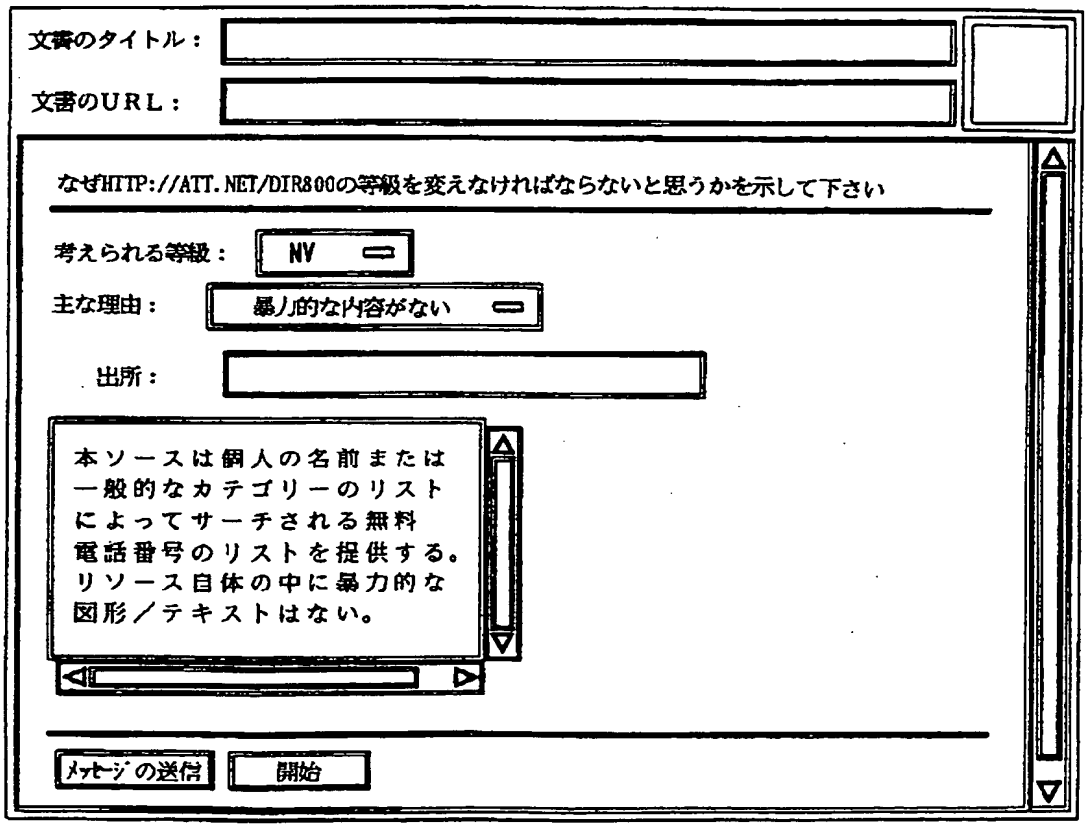
【図４】


文書のタイトル：
文書のURL：
NV
現在の等級の理由を見る時は、ここをクリックして下さい。
同意しない時は、ここをクリックして下さい。
800 ディレクトリ
カテゴリーによるブラウズ
a b c d e f g h i j k l m n o p q r s t u v w x y z
名前によるブラウズ
a b c d e f g h i j k l m n o p q r s t u v w x y z 0 1 2 3 4 5 6 7 8 9
ブラウズを開始する文字をクリックして下さい。
文字列サーチ
サーチ開始
フォームのクリア
サーチが反応しない。空白は「AND」を示す。
電話番号サーチ
サーチ開始
フォームのクリア
我々はあなたが毎日忙しいことを知っています。そのため我々は10年前にプリントされた800ディレクトリを作りました。その

【図５】



【図６】



フロントページの続き

(72)発明者　エリック　グロッス
アメリカ合衆国　07922　ニュージャーシィ，バークレイ　ハイツ，ノース　ロード
140